

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant:

Peter Szor

Assignee:

Symantec Corporation

Title:

SIGNATURE EXTRACTION SYSTEM AND METHOD

Serial No.:

10/611,472

Filed:

June 30, 2003

Group Art

2131

Examiner:

Unknown

Unit:

Docket No.:

SYMC1034

Monterey, CA December 5, 2003

Commissioner for Patents P.O. Box 1450 Alexandria, VA 22313-1450

INFORMATION DISCLOSURE STATEMENT UNDER §1.97(b)

Sir:

Pursuant to 37 C.F.R. §§ 1.56, 1.97 and 1.98, Applicant wishes to call the following documents (a copy of each is enclosed) to the attention of the Examiner:

U.S. PATENT DOCUMENTS:

U.S.	PATENT DOCUMENTS:				
	DOCUMENT NUMBER	DATE	NAME		
		03/12/02	Nachenberg		
1)	6,357,008		Hollander et al.		
2)	6,301,699	10/09/01			
	5,822,517	10/13/1998	Dotan		
3)		12/09/97	Nachenberg		
4)	5,696,822	12/00/1			
			•		

OTHER DOCUMENTS:

1)	Szor, P., "Attacks on WIN32", Virus Bulletin Conference, October 1998, Virus Bulletin Ltd., The Pentagon, Abingdon, Oxfordshire, England, pp. 57-84.
2)	Szor, P., "Memory Scanning Under Windows NT", Virus Bulletin Conference, September 1999, Virus Bulletin Ltd., The Pentagon, Abingdon, Oxfordshire, England, pp. 1-22.
3)	Szor, P., "Attacks on WIN32-Part II", Virus Bulletin Conference, September 2000, Virus Bulletin Ltd., The Pentagon, Abingdon, Oxfordshire, England, pp. 47-68.
4)	Chien, E. and Szor, P., "Blended Attacks Exploits, Vulnerabilities and Buffer-Overflow Techniques In Computer Viruses", Virus Bulletin Conference, September 2002, Virus Bulletin Ltd., The Pentagon, Abingdon, Oxfordshire, England, pp. 1-36.
5)	Buysse, J., "Virtual Memory: Window NT® Implementation", pp. 1-15 [online]. Retrieved on April 16, 2003. Retrieved from the Internet: <url:http: buyssej-term.pdf="" courses="" cs384="" papers19992000="" people.msoe.edu="" ~barnicks="">.</url:http:>
6)	Dabak, P., Borate, M. and Phadke, S., "Hooking Windows NT System Services", pp. 1-8 [online]. Retrieved on April 16, 2003. Retrieved from the Internet: <url:http: 06="" 2.html="" 356="" content="" www.windowsitlibrary.com="">.</url:http:>
7)	"How Entercept Protects: System Call Interception", pp. 1-2 [online]. Retrieved on April 16, 2003. Retrieved from the Internet: <url:http: kernelmode.asp="" products="" technology="" www.entercept.com="">. No author provided.</url:http:>
8)	"How Entercept Protects: System Call Interception", pg. 1 [online]. Retrieved on April 16, 2003. Retrieved from the Internet: <url:http: interception.asp="" products="" technology="" www.entercept.com="">. No author provided.</url:http:>
9)	Kath, R., "The Virtual-Memory Manager in Windows NT", pp. 1-11 [online]. Retrieved on April 16, 2003. Retrieved from the Internet: <url:http: dngenlib="" en-us="" html="" library="" msdn.microsoft.com="" msdn_ntvmm.asp?frame="true">.</url:http:>
10)	Szor, P. and Kaspersky, E., "The Evolution of 32-Bit Windows Viruses", Windows & .NET Magazine, pp. 1-4 [online]. Retrieved on April 16, 2003. Retrieved from the Internet: <url:http: articles="" print.cfm?articleid="8773" www.winnetmag.com="">.</url:http:>
11)	Szor, P., "The New 32-bit Medusa", Virus Bulletin, December 2000, Virus Bulletin Ltd., The Pentagon, Abingdon, Oxfordshire, England, pp. 8-10.

12)	Szor, P., "Shelling Out", Virus Bulletin, February 1997, Virus Bulletin Ltd., The Pentagon, Abingdon, Oxfordshire, England, pp. 6-7.
13)	McCorkendale, B. and Szor, P., "Code Red Buffer Overflow", Virus Bulletin, September 2001, Virus Bulletin Ltd., The Pentagon, Abingdon, Oxfordshire, England, pp. 4-5.
14)	Nachenberg, C., "A New Technique for Detecting Polymorphic Computer Viruses", University of California, Los Angeles, 1995
15)	"INFO: CreateFileMapping() SEC_* Flags", pp. 1-2 [online]. Retrieved on September 24, 2003. Retrieved from the Internet: <url:http: .microsoft.com:80="" 2="" 31.asp&nowebcontent="1" articles="" default.aspx?scid="http://support" kb="" q108="" support="" support.microsoft.com=""> No author provided.</url:http:>
16)	"CreateFileMapping", pp. 1-5 [online]. Retrieved on September 10, 2003. Retrieved from the Internet: <url:http: base="" createfilemapping.asp?frame="true" en-us="" fileio="" library="" msdn.microsoft.com=""> No author provided.</url:http:>

A PTO form 1449 listing these documents is enclosed.

U.S. PATENT APPLICATIONS (COPIES ENCLOSED):

	SERIAL NUMBER	FILING DATE	NAME
1)	10/360,341	02/06/03	Szor
2)	10/464,091	06/17/03	Szor
3)	10/681,623	10/07/03	Szor

Citation of the above documents shall not be construed as:

- 1. an admission that the documents are necessarily prior art with respect to the instant invention;
- 2. a representation that a search has been made, other than as described above; or
- 3. an admission that the information cited herein is, or is considered to be, material to patentability as defined in § 1.56(b).

The Commissioner is hereby authorized to charge any fees required for consideration of this Information Disclosure Statement, and to credit any overpayment of fees to Deposit Account No. 50-0553.

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage for First Class Mail in an envelope addressed to: Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313 1450 on December 5, 2003.

Attorney for Applicant

December 5, 2003

Date of Signature

Respectfully submitted,

Serge J. Hodgson

Attorney for Applicant

Reg. No. 40,017 (831) 655-0880

								Sheet	1 of 8
Form PTC	-1449				Atty Docke	et No.		Serial No).
SEVO	EVE					SYMC1034			472
- A	TURORI	MATION DISCLOS	TURE CITATIO	N	Applicant	(s)			
6 200	E.	MATION DISCLOS	CATION		Peter Sz	or			
HE SHE	Ž,				Filing Dat	:e		Group	
FEMT & TRA		several sheets			June 30,	2003		2131	
			v.s.	PATENT D	OCUMENTS				
EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME		CLASS	SUBCLASS	FILING IF APP	DATE ROPRIATE
	AA	6,357,008	03/12/02	Nachenbe	rg	713	200		
-	AB	6,301,699	10/09/01	Hollande	r et al.	717	4		
	AC	5,822,517	10/13/98	Dotan		395	186		
	AD	5,696,822	12/09/97	Nachenbe	rg	380	4		
	AE								
	AF								
,	AG								
	AH	·							
	AI								
	AJ								
	AK						1		
	<u> </u>		FOREIG	N PATENT	DOCUMENTS	}			-
								Tran	slation
		DOCUMENT NUMBER	DATE	COUNTRY		CLASS	SUBCLASS	YES	NO
	AL								
	AM								
	AN								
	AO								
	AP				-			Ì	
		OTHER DOCUME	NTS (Includin	g Author, T	itle, Date,	Pertinent P	Pages, Etc.)		
	AR	Szor, P., "A Virus Bullet 57-84.							
	AS	Szor, P., "M September 19 England, pp.	99, Virus Bu	ing Under illetin Lt	Windows 1 d., The I	VT", Virus Pentagon,	Bulletin Abingdon,	Confer Oxford	cence, lshire,

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant(s).

Date Considered

Examiner

	P E	
	(°)	MILE E
Form PTO-1449	ME O	C. C. Co.
	WENT 8	TRADELE
INFORM	TION DI	SCLOSURE

ΑJ ΑK

E CITATION

IN AN APPLICATION

Atty Docket No.	Serial No.
SYMC1034	10/611,472

Applicant(s)

Peter Szor Filing Date

Group

(Use several sheets if necessary)

June 30, 2003

2131

EXAMINER FILING DATE DOCUMENT NUMBER DATE NAME CLASS SUBCLASS INITIAL IF APPROPRIATE AA AB AC ΑD ΑE AF. AG AΗ ΑI

U.S. PATENT DOCUMENTS

FOREIGN PATENT DOCUMENTS

				Translation			
	DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	YES	ио
AL							
AM							
AN							
AO							
AP							

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

- Szor, P., "Attacks on WIN32-Part II", Virus Bulletin Conference, September 2000, Virus Bulletin Ltd., The Pentagon, Abingdon, Oxfordshire, England, pp. 47-68.
 - Chien, E. and Szor, P., "Blended Attacks Exploits, Vulnerabilities and AS Buffer-Overflow Techniques In Computer Viruses", Virus Bulletin Conference, September 2002, Virus Bulletin Ltd., The Pentagon, Abingdon, Oxfordshire, England, pp. 1-36.

Examiner

Date Considered

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant(s).

Sheet 3 of 8 1449 Serial No. Atty Docket No. SYMC1034 10/611,472 FORMATION DISCLOSURE CITATION Applicant(s) Peter Szor IN AN APPLICATION Filing Date Group June 30, 2003 2131 (Use several sheets if necessary) U.S. PATENT DOCUMENTS EXAMINER SUBCLASS FILING DATE DOCUMENT NUMBER DATE NAME CLASS INITIAL IF APPROPRIATE AA AB AC AD ΑE ΑF AG AΗ ΑI

FOREIGN PATENT DOCUMENTS

						Translation	
	DOCUMENT NUMBER	DATE	COUNTRY	CLASS	SUBCLASS	YES	МО
AL		_					
AM							
AN							
AO							
AP							

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

AR	Buysse, J., "Virtual Memory: Window NT® Implementation", pp. 1-15 [online]. Retrieved on April 16, 2003. Retrieved from the Internet: <url:http: buyssej-term.pdf="" courses="" cs384="" papers19992000="" people.msoe.edu="" ~barnicks="">.</url:http:>
 AS	Dabak, P., Borate, M. and Phadke, S., "Hooking Windows NT System Services", pp. 1-8 [online]. Retrieved on April 16, 2003. Retrieved from the Internet: <url:http: 06="" 2.html="" 356="" content="" www.windowsitlibrary.com="">.</url:http:>

Examiner

ΑJ ΑK

Date Considered

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant(s).

							ä	Sheet	4 of
Form PTO	-1449				Atty Docke	et No.		Serial No.	
E VCx	E vo					SYMC1034 10/			
PR Y	FOR	MATION DISCLOSU	RE CITATIO	N	Applicant((s)			
,00°	왕] 왕]	IN AN APPLICA	TION		Peter Sz	or			
					Filing Dat	:e		Group	
ENT & THE	(Use	several sheets if	necessary)		June 30,	2003		2131	
			v. s.	PATENT D	CUMENTS				
EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME		CLASS	SUBCLASS		DATE COPRIATE
	AA								
	AB								
	AC								
•	AD								
	AE								
•	AF								
. 	AG								
	AH								
	AI								
	AJ								
	AK								
-			FOREI	GN PATENT	DOCUMENTS	}			
								Trans	lation
-		DOCUMENT NUMBER	DATE	COUNTRY		CLASS	SUBCLASS	YES	по
	AL								
	AM								
	AN								
	AO								
	AP								
		OTHER DOCUMENT	rs (Includin	ng Author, Ti	itle, Date,	Pertinent Pa	ges, Etc.)		
	AR	"How Entercept Retrieved on F Internet: <url: kernelmode.asp</url: 	April 16, 3 http://www	2003. Ret w.entercep	rieved frot.com/pro	om the			e].
	AS	"How Entercept Retrieved on A Internet: <url: interception.a</url: 	April 16, : http://ww	2003. Ret w.entercep	rieved frot.com/pro	om the			
Examiner		I	Date Consi	dered					

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant(s).

		ME 08 1						Sheet	5 of 8
Form PTO-14 TO ENT & TRADE					Atty Docke	et No.		Serial No.	
		WI & WI			SYMC1034	<u>l</u>		10/611,4	72
נ	NFORN	MATION DISCLOS	URE CITATION		Applicant	(s)			
		IN AN APPLIC	ATION		Peter Sz	zor			
					Filing Dat	te		Group	
	(Use	several sheets i	f necessary)		June 30,	2003		2131	
			υ.s. i	PATENT D	OCUMENTS				
EXAMINER INITIAL		DOCUMENT NUMBER	DATE	NAME		CLASS	SUBCLAS	S FILING	
	AA								
	AB								
•	AC								
	AD								
•	AE								
	AF								
	AG	""							
	AH								
	AI								
	AJ			-					
	AK							·	
			FOREIGN	PATENT	DOCUMENTS	3			
								Trans	lation
		DOCUMENT NUMBER	DATE	COUNTRY		CLASS	SUBCLAS	S YES	ио
	AL								
	AM								
	AN		,						
	AO								
	AP								
		OTHER DOCUME	NTS (Including	Author, T	itle, Date,	Pertinent Pa	ıges, Etc.)	
	AR	AR Kath, R., "The Virtual-Memory Manager in Windows NT", pp. 1-11 [online]. Retrieved on April 16, 2003. Retrieved from the Internet: <url:http: dngenlib="" en-="" html="" library="" msdn="" msdn.microsoft.com="" ntvmm.asp?frame="true" us="">.</url:http:>							
	AS	Szor, P. and Kaspersky, E., "The Evolution of 32-Bit Windows Viruses", Windows & .NET Magazine, pp. 1-4 [online]. Retrieved on April 16, 2003. Retrieved from the Internet: <url:http: articles="" print.cfm?articleid="8773" www.winnetmag.com="">.</url:http:>							
Examiner			Date Conside	ered					

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant(s).

										
松 					Atty Docket No.			Serial No.		
(4) E					SYMC1034 10/611,472					
INEGRMATION DISCLOSURE CITATION					Applicant(s)					
ON ENIS TRE	Ž	IN AN APPLICA	ATION		Peter Szor					
MENT & TRA					Filing Dat	:e		Group		
	(Use	several sheets in	f necessary)		June 30,	2003		2131		
			U.S. I	PATENT D	OCUMENTS					
EXAMINER INITIAL			DATE	NAME		CLASS	CLASS SUBCLASS		DATE OPRIATE	
	AA							-		
	AB									
	AC			1						
	AD			 		-			***	
-1	AE								=	
	AF									
•	AG									
	AH		1							
	AI			1						
	AJ			1						
	AK									
			FOREIGN	PATENT	DOCUMENTS	}		<u>, </u>		
								Trans	lation	
		DOCUMENT NUMBER	DATE	COUNTRY		CLASS	SUBCLASS	S YES	ио	
	AL									
	AM									
	AN									
	AO									
	AP									
		OTHER DOCUMEN	TTS (Including	Author, T:	itle, Date,	Pertinent Pa	ges, Etc.)	•	
	AR Szor, P., "The New 32-bit Medusa", Virus Bulletin, December 2000, Virus Bulletin Ltd., The Pentagon, Abingdon, Oxfordshire, England, pp. 8-10.								rus .0.	
	AS	Szor, P., "Shelling Out", Virus Bulletin, February 1997, Virus Bulletin Ltd., The Pentagon, Abingdon, Oxfordshire, England, pp. 6-7.								
Examiner Date Considered				ered						
EXAMINER:	Initia	al if reference co	onsidered, wheth	er or not	citation is	in conforma	nce with	MPEP 609; di	raw line	

EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant(s).

20 m PTO, 1449				Atty Docke	et No.	Serial No.				
INEXTRACTION DISCLOSURE CITATION IN AN APPLICATION				SYMC1034 10/611,472						
08	O INEORMATION DISCLOSURE CITATION				Applicant(s)					
₩		IN AN APPLIC	ATION		Peter Szor					
WEIT & T					Filing Dat	:e		Group		
	(Use	several sheets i	f necessary)		June 30,	2003		2131	2131	
U.S. PATENT DOCUMENTS										
EXAMINER INITIAL		DOCUMENT NUMBER DATE NAME				CLASS SUBCLA		FILING IF APPR		
	AA									
	AB									
	AC									
	AD								-	
	AE									
	AF									
	AG									
	AH									
	AI									
	AJ									
	AK									
			FOREIGN	PATENT	DOCUMENTS	8				
							Trans	lation		
		DOCUMENT NUMBER	DATE	DATE COUNTRY		CLASS	SUBCLAS	S YES	NO	
	AL									
	AM									
	AN									
	AO									
	AР									
OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)										
	AR McCorkendale, B. and Szor, P., "Code Red Buffer Overflow", Virus Bulletin, September 2001, Virus Bulletin Ltd., The Pentagon, Abingdon, Oxfordshire, England, pp. 4-5.									
	AS Nachenberg, C., "A New Technique for Detecting Polymorphic Computer Viruses", University of California, Los Angeles, 1995									
Examiner			Date Considered							
EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant(s).										

				 		 				
Form PTO-1449				Atty Docket No. Serial No.						
E				SYMC1034 10/611,472						
INFORMATION DISCLOSURE CITATION				Applicant(s)						
D JUL	IN AN APPLICATION				Peter Szor					
W O	E PORTO				Filing Dat	:e	Group	Group		
\(\sigma_{\sigma}\)	Use several sheets if necessary)				June 30,	2003		2131		
U.S. PATENT DOCUMENTS										
EXAMINER INITIAL		DOCUMENT NUMBER	R DATE NAME			CLASS	SUBCLAS		FILING DATE IF APPROPRIATE	
	AA									
	AB									
	AC									
	AD									
	AE									
	AF									
	AG									
	AH	-								
	AI									
	AJ									
	AK		<u> </u>		· ·					
			FOREIGN	PATENT	DOCUMENTS					
Translatio								lation		
		DOCUMENT NUMBER	DATE	COUNTRY		CLASS	SUBCLAS	S YES	NO	
	AL									
	AM									
	AN									
	AO									
	AP									
OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)										
	AR "INFO: CreateFileMapping() SEC_* Flags", pp. 1-2 [online]. Retrieved on September 24, 2003. Retrieved from the Internet: <url:http: default.aspx?scid="http://support.Microsoft.com:80/support/kb/articles/Q108/2/31.asp&NoWebContent=1" support.microsoft.com=""> No author provided.</url:http:>									
	AS "CreateFileMapping", pp. 1-5 [online]. Retrieved on September 10, 2003. Retrieved from the Internet: <url:http: base="" createfilemapping.asp?frame="true" en-us="" fileio="" library="" msdn.microsoft.com=""> No author provided.</url:http:>							/en-		
Examiner	Examiner Date Considered									
EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609; draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant(s).										